component. In view of this, in this work a method of object identification of critical information infrastructure is developed, which gives ability to determine the critical infrastructure elements, their mutual influence and influence on functional operations of the critical aviation information system. This method, as well as a software application developed on its basis, can be used for identification the objects of critical information infrastructure in different industries.

Keywords: critical infrastructure, critical information infrastructure, critical aviation information systems, object identification of critical information infrastructure, civil aviation.

Сергій Олександрович Гнатюк, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій, Національний авіаційний університет, Київ, Україна.
E-mail: S.Gnatyuk@nau.edu.ua.
Вікторія Миколаївна Сидоренко, асистент кафедри безпеки інформаційних технологій, Національний авіаційний університет, Київ, Україна.
E-mail: v.sydorenko@ukr.net.
Василь Миколайович Кінзерявий, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій, Національний авіаційний університет, Київ, Україна.
E-mail: V.Kinzeryavyy@gmail.com.

Сергей Александрович Гнатюк, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий, Национальный авиационный университет, Киев, Украина.
Виктория Николаевна Сидоренко, ассистент кафедры безопасности информационных технологий, Национальный авиационный университет, Киев, Украина.
Василий Николаевич Кинзерявый, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий, Национальный авиационный университет, Киев, Украина.

Serhii Hnatiuk, candidate of technical sciences, associate professor, associate professor of IT-security academic department, National Aviation University, Kyiv, Ukraine.
Viktoriia Sydorenko, assistant of IT-security academic department, National Aviation University, Kyiv, Ukraine.
Vasyl Kinzeriavyi, candidate of technical sciences, associate professor, associate professor of IT-security academic department, National Aviation University, Kyiv, Ukraine.

УДК 004.056.53:621.391

ІГОР ЯКОВІВ

ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, КОНЦЕПТУАЛЬНА МОДЕЛЬ КІБЕРПРОСТОРУ І КІБЕРБЕЗПЕКА

Семантичні невизначеності між базовими поняттями у галузі кібербезпеки значно звужують діапазон і знижують результативність наукових досліджень щодо методів аналізу і прогнозування, наприклад, APT кібератак або розробки комплексів захисту на основі формальних моделей доказу їх ефективності. Напрям можливого подолання проблеми – розробка концептуальної моделі кібепростору і кібербезпеки, що дозволяє знижувати рівень можливих невизначень при описі різноманітних складних ситуацій у кіберпросторі завдяки застосуванню спеціальних інструментів термінологічної, графічної і математичної формалізації. Початок досліджень – обране твердження: фізичну основу кіберпростору складають інформаційно-телекомунікаційні системи (ІТС). Аналіз інформаційних процесів

таких систем було проведено на основі застосування атрибутивно-трансферного підходу до сутності інформації. Він визначає "інформацію" як таки набути властивості (атрибути) об'єкту, що відображають властивості іншого об'єкту. Електронні пристрої та фізичні середовища передачі сигналів складають технологічну основу ІТС. Дискретні електронні та електромагнітні сигнали, що циркулюють між електронними пристроями, дозволяють формувати інформацію, перетворювати її та передавати у просторі на різну відстань. За допомогою різних наборів електронних пристроїв і сигналів в ІТС реалізуються різноманітні технології обробки інформації. Вони забезпечують користувачів ІТС різними інформаційними послугами (сервісами). Користувачами ІТС можуть бути як люди, так і технічні системи (пристрої). За результатами аналізу розроблено концептуальну модель кіберпростору і кібербезпеки. Модель складають: 1) набір взаємоузгоджених базових термінів, що відображають сутність інформаційних процесів в ІТС і їх складових. Завдяки цих термінів синтезовані визначення для термінів "кіберпростір" і "кібербезпека"; 2) графічна модель кіберпростору, що пояснює співвідношення його складових; 3) математична модель кіберпростору – набір теоретико-множних уявлень, що конкретизують характер взаємовідношень між компонентами кіберпростору. Завдяки моделі кіберпростору було розроблено математічні критерії кібербезпеки для сегменту кіберпостору. Модель також дозволяє значно спростити процес сценарного аналізу APT атак або складних процесів захисту у кіберпросторі.

Ключові слова: APT атака, інформаційно-телекомунікаційна система, кіберпростір, кібербезпека, семантична невизначеність термінів, концептуальна модель кіберпостору, інформаційні відношення у кіберпросторі, формальні критерії кібербезпеки, сценарний аналіз APT атак.

Вступ. Активізація процесів політичної та економічної інтеграції України з Європейським Союзом значно підвищила зацікавленість в питаннях забезпечення кібернетичної безпеки (кібербезпеки) в сегменті національної інформаційної інфраструктури. Під терміном *кібербезпека*, як правило, розуміється забезпечення властивостей інформації (конфіденційність, цілісність, доступність та інші) в *кіберпросторі* [1]. У світовій практиці широке використання термінів "кіберпростір*"* ("cyberspace") і "кібербезпека" ("cybersecurity", "cyberspace security") почалося з середини минулого десятиліття (в 2005-2007 роках). Вони все частіше стали застосовуватися там, де раніше використовувалися терміни "безпека систем інформаційних технологій" ("Information Technology Systems security", ITS security) і "комп'ютерна безпека" ("computer security") [10].

У нашій країні з кінця 90-х років минулого століття для позначення розподілених електронних систем, які об'єднують в собі комп'ютерні технології та технології електрозв'язку, застосовувався термін "інформаційно-телекомунікаційні системи" (ІТС). За минулі роки в рамках формування та реалізації державної політики захисту інформації в ІТС розроблено значну кількість (понад 200) нормативно-правових документів, які знайшли широке застосування. Очевидно, що нормотворча діяльність в сфері забезпечення кібернетичної безпеки України, що активно проводиться в даний час, повинна враховувати необхідність гармонізації нових регулюючих актів з раніше напрацьованими документами з захисту інформації. Основою для такої гармонізації може стати формалізована модель кіберпростору, що відображає в собі як аспекти застосування ІТС в різних процесах управління, так і ключові аспекти забезпечення кібербезпеки.

Така модель також має допомогти зменшити рівень невизначеності в розумінні суті кіберпростору. Це дозволяє розширити рамки досліджень складних процесів у галузі забезпечення кібербезпеки. Наприклад, перспективними виглядає напрям розробки комплексу засобів сценарного аналізу нового класу кіберзагроз – APT атак (англ. "Advanced Persisten Threat" – "розвинена стійка загроза"; цільова або таргетована кібератака). Конструктивним буде такий підхід, що дозволяє з єдиних теоретичних позицій провести формалізований аналіз всіх фаз такої кібератаки, що значно відрізняються за цілями та методами реалізації.

Виклад основного матеріалу дослідження.

1. Кіберпростір як фізичне середовище: аналіз досліджень, постановка завдання. Ключовим терміном для розуміння сутності "кібербезпеки" є "кіберпростір". Зазвичай його пов'язують з:

– глобально розподіленими системами, що реалізовують цифрові комп'ютерні технології обробки інформації;

– віртуальним середовищем на основі цих систем, в якому можуть існувати видумані активні об'єкти (різноманітні герої комп'ютерних ігор і цифрової анімації, симуляційні моделі та інше). Ці інформаційні об'єкти, що існують тільки в комп'ютерах, здатні здійснювати реальний сенсорний вплив на психіку людини (візуальний, звуковий та іншій);

– можливістю здійснювати приховані (анонімні) інформаційні впливи на людей і різні пристрої;

– відсутністю "територіальних кордонів" при комунікаціях людей різних держав (відсутність "кіберкордонів").

Так, наприклад, в міжнародному стандарті "ISO/IEC 27032: 2012 Information technology. Security techniques. Guide lines for cybersecurity" пропонується наступне визначення: "кіберпростір – це складне середовище, сформоване в Інтернеті в результаті взаємодії людей, програмного забезпечення і послуг за допомогою технологічних пристроїв і мереж, підключених до нього, і яке не існує в будь-якій фізичній формі". Таке визначення, по-перше, обмежує кіберпростір ситуаціями використання комп'ютерних технологій тільки в рамках Інтернет. По-друге, відмовляючи йому в наявності фізичної форми, позбавляє його матеріальності і, відповідно, відмовляє в можливості проведення об'єктивного (інструментального) контролю його станів. Останнє є дуже критичним для забезпечення кібербезпеки.

Багато дослідників все ж представляють кіберпростір таким середовищем, яке утворено цілком фізичними системами і мережами [2], [3]. Такий підхід дозволяє говорити і про існування фізичних національних "кіберкордонів", які формуються відповідними інженерно-технічними комплексами. В рамках цих кордонів може здійснюватися як фізичний контроль технічного обладнання, так і інформаційних потоків, які перетинають ці межі [4].

У національному законодавстві здебільшого додержуються позицій фізичних засад: "кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних" [7]. Але застосування терміну "середовище (віртуальний простір)" без визначення його фізичної сутності не дозволяє, на думку автора, подолати іншу невизначеність щодо характеру взаємозв'язку між поняттями "кіберпростір" і "сумісні (з'єднані) комунікаційні системи " та "електронні комунікації".

Ці та ряд інших семантичних невизначеностей між поняттями у галузі забезпечення кібербезпеки значно звужують діапазон і знижують результативність наукових досліджень щодо методів аналізу і прогнозування, наприклад, APT кібератак [8], або розробки комплексів захисту на основі формальних моделей доказу їх ефективності. Один із напрямів можливого подолання проблеми – розробка концептуальної моделі кібепростору і кібербезпеки, що дозволяє знижувати рівень можливих невизначень при описі різноманітних складних ситуацій у кіберпросторі завдяки застосуванню спеціальних інструментів термінологічної, графічної і математичної формалізації.

За початкову позицію на шляху розробки концептуальної моделі було обрано наступне твердження: фізичну основу кіберпростору складають інформаційно-телекомунікаційні системи. Формування формалізованої моделі кіберпростору доцільно почати з аналізу сутності інформаційних процесів в цих системах.

2. Аналіз інформаційних процесів в інформаційно-телекомунікаційних системах. Під інформаційно-телекомунікаційною системою в вітчизняних нормативних документах розуміють сукупність інформаційних (автоматизованих) систем (ІС) і телекомунікаційних систем (ТС), які в процесі обробки інформації діють як єдине ціле [5]. У свою чергу, інформаційна (автоматизована) система (ІС, АС) – це організаційно-технічна система, в якій реалізується технологія обробка інформації (ТОІ) з використанням технічних і програмних засобів [5]. Телекомунікаційна система визначається як сукупність технічних і програмних засобів для обміну інформацією шляхом передачі, випромінювання або прийому її у вигляді сигналів, знаків, змінюваних або незмінних зображень або іншим способом [5].

Для аналізу інформаційних процесів ІТС, перш за все, необхідно визначитися з сутністю інформації. Пропонується зупинитися на атрибутивно-трансферному підході [6], за яким "інформація" визначається як властивості (атрибути) об'єкту, що відображають властивості іншого об'єкту (тобто інформація - результат трансферту властивостей від одного об'єкта до іншого). Інформація завжди пов'язана зі своїм носієм, тобто тим фізичним об'єктом, який є носієм відображених властивостей.

З урахуванням такого підходу можна більш детально розглянути інформаційні процеси. Обробка інформації (її зберігання, перетворення, передача і інші операції) в ІТС здійснюється за допомогою електронних, радіоелектронних і/або оптоелектронних технічних пристроїв. Такі пристрої складають загальну технологічну основу для інформаційних процесів, як в інформаційних, так і в телекомунікаційних системах. Робота цих пристроїв заснована на використанні можливостей електромагнітної взаємодії частинок з електричними зарядами. Інформація в сучасних ІТС представляється у вигляді різних комбінацій з двох значень (0 і 1) елементарної одиниці інформації, яка називається біт. Носіями такої двійковій одиниці в ІТС є різні електромагнітні дискретні (цифрові) сигнали (електричні, оптичні, радіосигнали). На відміну від аналогових (безперервних) сигналів дискретні сигнали приймають тільки кінцеве число можливих значень (наприклад, 2, 4, 8, 16, 32). Це дозволяє будь-які відомості (тобто комбінацію одиниць і нулів) представити сукупністю електромагнітних (електричних, оптичних, радіо) сигналів, що переносять інформацію в просторі. Сигнали електронних пристроїв також беруть участь в процесах запису/зчитування інформації з елементів пам'яті. За їх допомогою по заданих обчислювальним алгоритмам також здійснюються різні перетворення одних двійкових комбінацій в інші (перетворення інформації).

За допомогою застосування наборів різних електронних пристроїв і сигналів в ІТС можуть бути реалізовані різноманітні технології обробки інформації (ТОІ). Вони забезпечують користувачів ІТС різними інформаційними послугами (сервісами). Користувачами таких послуг можуть бути як люди, так і технічні системи (пристрої). Між користувачами ІТС можуть виникати різні інформаційні відносини на основі застосування між ними різних сервісів ІТС.

3. Безпека інформації в ІТС. При аналізі інформаційних процесів в ІТС важливо уточнити сутність терміна "безпека інформації". В рамках замовленого інформаційного сервісу користувач пред'являє вимоги до інформаційного продукту (тобто до інформації, яка формується ТОІ). Наприклад, при передачі інформації відправник часто зацікавлений в її доставці без порушення конфіденційності та/або цілісності. В іншому випадку, при зверненні до необхідного інформаційного ресурсу користувач зацікавлений в надійній реалізації його права доступу до інформації, тобто забезпечення доступності. Ці та безліч інших можливих прикладів свідчать про існування зацікавленості користувачів ІТС в наданні їм послуг з такою якістю, яка може бути виражена у вигляді набору властивостей інформаційного продукту. Вплив на ІТС різних негативних факторів (природних, техногенних, людських та інших) може призводити до порушення цих властивостей, тобто порушення якості інформаційного продукту. З позицій організації ефективної протидії серед усіх негативних впливів найбільшу зацікавленість представляють навмисні дії людини, які при сучасному рівні розвитку технологій можуть носити досить складний, мало прогнозований характер. Вони постійно удосконалюються. Для їх успішної реалізації, як правило, необхідні сильна мотивація,

високий рівень знань механізмів роботи ІТС та досвід практичної діяльності в сфері цифрових технологій. З огляду на більш значну передбачуваність (в першу чергу, статистичну) інших несприятливих факторів їх доцільно пов'язувати з терміном "надійність ІТС". Так, наприклад, природний вихід з ладу магнітного накопичувача призводить порушення доступності інформації. Однак, знання середнього часу напрацювання на відмову для цього пристрою, дозволяє ще на етапі розробки ІТС запланувати дієві заходи щодо резервування інформації.

Виходячи з вищевказаних позицій, пропонується уточнити термін "безпека інформації ІТС" і розуміти під ним такий стан ІТС, який забезпечує задані властивості інформаційного продукту в умовах навмисних несприятливих впливів на ІТС. У свою чергу, через цей термін можна визначити і наступний: "захист інформації в ІТС" – *це дії, спрямовані на досягнення і підтримання безпеки інформації ІТС.*

Додатково слід зазначити, що серед властивостей самої ІТС слід виділяти такі, використання яких зловмисником може призвести до порушення безпеки інформації. Такі властивості прийнято називати "уразливостями ІТС". Уразливість в сукупності з потенційним несприятливим впливом прийнято називати "загрозою". Загрозу, яка реалізована або перебуває в стадії реалізації, прийнято називати "атакою".

4. Властивості інформації, що визначають її безпеку. У рамках проведеної формалізації необхідно уточнити перелік властивостей інформації, через які визначається її безпека в ІТС.

Історично першими широкого поширення набули телекомунікаційні системи, в яких основною послугою є передача інформації (обмін інформацією). Ця послуга і визначила основні властивості, що пред'являються до інформації в аспекті її безпеки. Тривалий час безпека інформації визначалася через забезпечення таких властивостей як конфіденційність, цілісність, доступність (далі – К, Ц, Д). З появою, розвитком і поширенням інформаційних систем (автоматизованих систем) ситуація з вимогами до інформації змінилася. Застосування комп'ютерів і інших цифрових електронних пристроїв значно розширило спектр інформаційних послуг, що надаються. Це, в свою чергу, призвело до розширення необхідних властивостей інформаційного продукту. Поняття "безпека інформації" стали також пов'язувати із забезпеченням актуальності, достовірності і деяких інших властивостей інформації. Тут слід зазначити нову особливість розглянутих властивостей, яка більш чітко проявляється в рамках атрибутивно-трансфертного підходу до сутності інформації. Забезпечення К, Ц, Д не пов'язано з семантикою вихідної інформації і залежить тільки від коректної реалізації сервісів її передачі, зберігання, поширення і деяких інших. У той же час, забезпечення актуальності і достовірності також залежить і від семантики (змісту) вихідної інформації. Якщо ця семантика не відповідає актуальності і достовірності подій, які відображаються, то навіть коректні сервіси ІТС не забезпечать ці властивості інформаційного продукту.

Додатково слід також підкреслити те, що з урахуванням широкого застосування в ІТС сервісів перетворення інформації на основі заданих обчислювальних алгоритмів, актуальною стає необхідність врахування і властивості коректності реалізації заданого алгоритму перетворень (далі – коректність перетворень даних). Безліч відомих загроз пов'язано з порушенням алгоритму перетворень або з його повною заміною.

Як правило, необхідні властивості визначаються на етапі формування політики безпеки інформації для ІТС.

5. Концептуальна модель кіберпростору і кібербезпеки. Для розуміння сутності кіберпростору важливо також проаналізувати аспект його сприйняття у порівнянні зі звичайним фізичним простором. У звичайному просторі людина сприймає світ через безпосередні контакти з іншими об'єктами (смак, дотик), або – на відстані (зір, слух і нюх). Дистанційне сприйняття здійснюється через природні носії інформації (сонячне світло, акустичні коливання, хімічні сполуки) і обмежується кордонами сприйняття, які залежать від можливостей органів чуття. Поява мови та письма значно розширило ці межі. Однак ці два канали засновані на наявності посередників між подією і суб'єктом пізнання. Інтерпретація посередниками переданої інформації часто призводить до порушення її достовірності. Наслідок цього – спотворене сприйняття світу.

Застосування інформаційно-телекомунікаційних технологій не тільки значно розширює межі віддаленого сприйняття, але і збільшує можливості людини в аналізі прийнятої інформації і формуванні нових знань. В таких умовах навіть на інтуїтивному рівні виникає потреба асоціювати “нові можливості в фізичному просторі” і “комп’ютерні (кібернетичні) технології” в рамках нового ментального об’єкта, який назвали “кіберпростір”.

Таким чином, проведений вище аналіз інформаційних процесів ІТС (пункти 2-6) дозволив уточнити такі поняття: “інформація в ІТС”; “технологія електронної (цифрової) обробки інформації”; “інформаційний сервіс ІТС”; “інформаційний продукт” і його якість; “користувачі ІТС”; “інформаційні відносини” між користувачами ІТС; властивості і безпека інформації ІТС; взаємозв'язок “людина – фізичний простір – ІТС – кіберпростір”.

Результати аналізу дозволяють сформулювати наступний набір взаємоузгоджених визначень (термінологічна формалізація).

Кіберпростір – це сукупність інформаційних відносин між користувачами ІТС, які формуються за допомогою послуг (сервісів) цих систем.

Пояснюючі визначення:

Інформація – це властивості (атрибути), що перенесені (трансферт) з одного об’єкта на інший.

Носій інформації – об’єкт, в якому відображені властивості іншого об’єкту.

Користувач інформації ІТС – це людина або технічний об’єкт (система), який використовує інформаційний продукт ІТС в своїх інтересах (цілях).

Інформаційний продукт – це інформація із заданими користувачем властивостями, яка формується інформаційним сервісом (послугою).

Інформаційний сервіс (послуга) – це сукупність дій з вихідною інформацією з метою формування інформаційного продукту із заданими властивостями.

Властивості інформації – це ті якості інформації, які потрібні користувачу інформації.

Інформаційне відношення – це сукупність обраного інформаційного сервісу, вихідної інформації і сформованого інформаційного продукту.

Результат подальшої графічної формалізації вербальної моделі кіберпростору представлений на рис. 1.

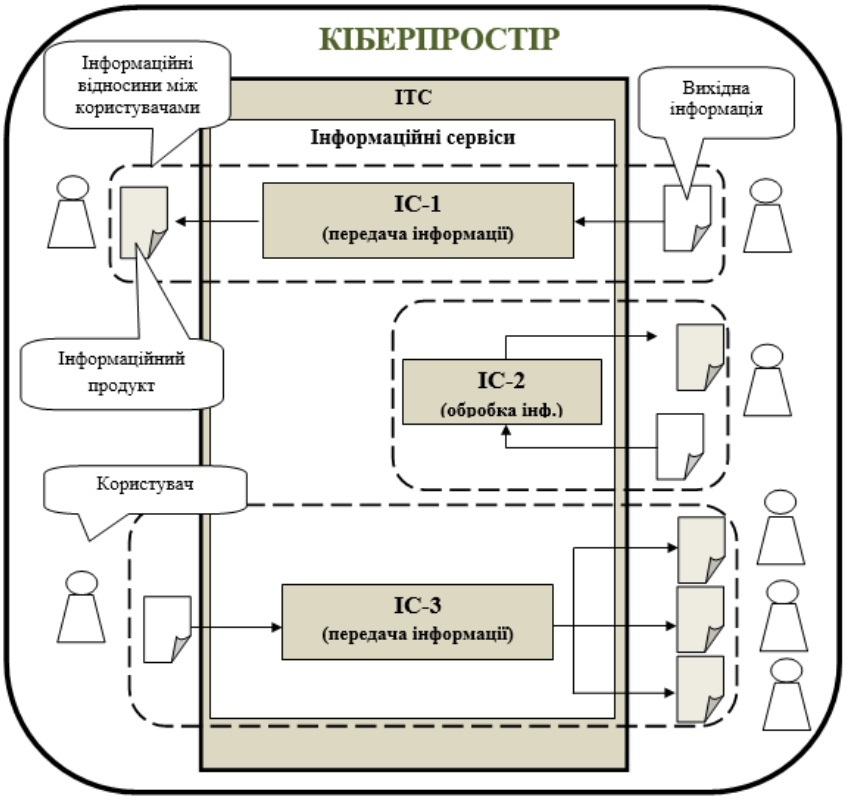

Рисунок 1 – Графічна формалізація вербальної моделі кіберпростору

Таке представлення кіберпростору дозволяє визначити наступне: "***кібербезпека*** – це стан інформаційно-телекомунікаційних систем, при якому навмисні несанкціоновані дії у кіберпросторі не порушують властивості інформаційних продуктів для користувачів цих систем".

Примітка:

1. Інтереси користувачів виражаються в заданих властивостях інформаційного продукту.
2. Найбільш відомі властивості інформації, які забезпечуються в ІТС:

конфіденційність; цілісність; доступність; достовірність; актуальність та інші.

3. Об'єкти кіберзахисту у кіберпросторі:
   - інформаційно-телекомунікаційні системи (ІТС);
   - інформаційні ресурси ІТС (інформаційні продукти, проміжна і технологічна інформація);
   - інформаційні сервіси ІТС;
   - користувачі ІТС.

6. Математичне представлення кіберпростору і кібербезпеки. Наданий вище набір термінів, суті яких узгоджені з допомогою прийнятих понять і відповідного графічного представлення, дозволяє усунути ряд невизначеностей в процесі аналізу актуальних проблем забезпечення кібербезпеки. Подальше зниження рівня невизначеностей може бути досягнуто через математичне представлення понять кіберпростору і кібербезпеки.

Розглянемо сегмент кіберпростору, який визначається інформаційно-телекомунікаційною системою ITS. У цьому випадку ця система може бути представлена у вигляді кінцевої множини

$$ITS = \{IA_i\},\ i=1,\ldots,I \tag{1}$$

де: IA_i – це i-те інформаційне відношення (Information Attitude , IA);

I – кількість інформаційних відношень (потужність множини) на етапі спостереження тривалістю T.

В свою чергу кожне інформаційне відношення може бути представлене через впорядковану трійку елементів наступним чином

$$IA_i = (In_i^*, f_i, In_i), \tag{2}$$

де In_i – вхідна інформація i-того сервісу;

f_i – i-тий сервіс;

In_i^* – інформаційний продукт, який формується i-тим сервісом.

Взаємозв'язок між елементами i-того інформаційного відношення може бути відображений у вигляді наступного представлення

$$In_i^* = f_i(In_i). \tag{3}$$

Таким чином, сегмент кіберпростору на основі конкретної *ITS* може бути представлений у вигляді (1)-(3). Для формального представлення стану кібербезпеки цього сегменту необхідно представити властивості інформаційного продукту In_i^* в кожному інформаційному відношенні IA_i. З цією метою виділимо алфавіт властивостей A, які користувач *ITS* може вимагати до інформаційного продукту In_i^* в рамках інформаційного відношення IA_i:

$$A = \{a_n\},\ n=1,..,N. \tag{4}$$

де a_n – одна із заданих властивостей;

N – кількість властивостей (потужність множини).

Тоді для кожного поточного інформаційного відношення можна виділити наступний набір властивостей:

$$A_i = \{a_{n,j}^{(i)}\} \subset A,\ j = 1,..,J, \tag{5}$$

де $a_{n,j}^{(i)}$ – n-та властивість із алфавіту A, що задана користувачем в рамках інформаційного відношення IA_i;

j – поточний номер властивості в наборі властивостей A_i, потужність якого J.

Нехай властивість $a_n^{(i)}$ може приймати одне з декількох можливих значень $v_k^{(n)} \in V_n = \{v_k^{(n)}\}$, тобто користувач може задати вимогу до інформаційного продукту в рамках IA_i інформаційного відношення:

$$a_n^{(i)} = v_k^{(n)}. \quad (6)$$

Так як заданих властивостей може бути декілька, то вони можуть бути представлені вектором

$$\boldsymbol{v}_i = (v_{1.}, \ldots, v_j, \ldots, v), \quad (7)$$

де v_j – задане значення j-тої властивості в наборі властивостей A_i.

Завдяки цьому надається можливість формально описати критерії кібербезпеки інформаційного відношення сегмента кіберпростору, сформованого на основі сервісів інформаційно-телекомунікаційної системи ITS. Для цього введемо *функцію кібербезпеки інформаційного відношення CyberSecurity (.)*, яка задається наступним чином

$$CyberSecurity(IA_i) = \begin{cases} 1\ (\textit{кібербезпека забезпечена}),\ \textit{якщо}\ v_i^* = v_i; \\ 0\ (\textit{кібербезпека відсутня}),\ \textit{якщо}\ v_i^* \neq v_i, \end{cases} \quad (8)$$

де v_i – вектор заданих значень властивостей інформаційного продукту;

v_i^* – вектор отриманих значень властивостей інформаційного продукту.

Зрозуміло, що критерієм забезпечення кібербезпеки всього сегмента кіберпростору на основі всіх актуальних послуг *ITS* буде виконання заданих вимог в рамках всіх інформаційних відносин, тобто:

$$CyberSecurity(ITS) = CyberSecurity(IA_1)\&CyberSecurity(IA_2)\&\ldots\&CyberSecurity(IA_I) = 1. \quad (9)$$

Приклад. Нехай ІТС повинна забезпечити наступні сервіси:

1) передачу одного файлу з вимогами забезпечення конфіденційності (*confidentiality*) та цілісності (*integrity*). Тобто задано інформаційне відношення IA_1;

2) перетворення іншого файлу за допомогою заданої програми за вимоги коректності її виконання (correctness). Тобто задано інформаційне відношення IA_2.

Для *сервісу передачі файлу даних* відповідно до (7) задані властивості будуть відображені наступним вектором

$$\boldsymbol{v}_1 = (v_{conf} = 1,\ v_{integrity} = 1).$$

Для сервісу *перетворення даних файлу* задані властивості будуть відображені наступним вектором

$$\boldsymbol{v}_2 = (v_{\text{correctness}} = 1).$$

Кибербезпека заданого сегменту кіберпростору буде забезпечуватися коли для любих несанкціонованих навмисних дій буде виконуватися наступна умова

$$CyberSecurity(ITS) = CyberSecurity(IA_1)\&CyberSecurity(IA_2) = 1,$$

тобто вектори заданих та отриманих значень властивостей інформаційних продуктів у кожному інформаційному відношенні мають співпадати (принцип «що хотіли, те й отримали»)

$$\boldsymbol{v}_1^* = \boldsymbol{v}_1;\ \boldsymbol{v}_2^* = \boldsymbol{v}_2.$$

Таким чином математична модель кіберпростору (1) - (7) і критерії кібербезпеки (8), (9) доповнюють надані раніше результати термінологічної і графічної формалізації.

Висновки. Ряд семантичних невизначеностей між поняттями у галузі забезпечення кібербезпеки значно знижують результативність наукових досліджень щодо:

– методів аналізу і прогнозування складних ситуацій у цієї галузі (наприклад, APT атак);

– розробки комплексів захисту на основі формальних моделей доказу їх ефективності.

За результатами аналізу сутності інформаційних процесів у інформаційно-телекомунікаційних системах і їх безпеки розроблено концептуальну модель (парадигму) кіберпростору і кібербезпеки. Модель складають:

1) набір взаємоузгоджених термінів, що відображають сутність інформаційних процесів в ІТС. За допомогою цього набору надається визначення термінів *кіберпростір* і *кібербезпека*;

2) графічна модель кіберпростору, що пояснює співвідношення його складових: ІТС, інформаційні сервіси, інформаційний продукт, користувачі ІТС, інформаційні відношення, безпека кіберпростору;

3) математична модель кіберпростору, що дозволяє за допомогою апарату теоретико-множних уявлень конкретизувати характер взаємовідношень між компонентами кіберпростору.

За допомогою концептуальної моделі отримані формальні критерії кібербезпеки у сегменті кіберпостору, що сформований на основі сервісів заданої інформаційно-телекомунікаційної системи.

У разі представлення компонентів кіберпростору у вигляді об'єкту управління можливе узгоджене застосування додаткового набору засобів формалізації інформаційного процесу управління кіберсистеми [9]. Наприклад, користувачем ІТС є технологічний процес (транспортна система, мережа енергопостачання, процес збагачення уранової руди та інше). У цьому разі ІТС і об'єкт управління можливо розглядати як кібернетичну систему, поведінка якої представляється послідовністю різних фаз об'єкту управління, що визначаються політикою управління. Математична формалізація цього процесу на основі запропонованого набору засобів значно спрощує процес сценарного аналізу APT атак.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] International Organization for Standardization. (2012, July 16). ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity.

[2] F. Kramer, S. Starr, and L. Wentz, *Cyberpower and National Security*. Washington, USA: Potomac Books, 2009.

[3] J.B. Sheldon, "Deciphering cyberpower strategic purpose in peace and war", *Strategic Studies Quarterly*, vol. 5, no. 2, pp. 95-112, 2011.

[4] Д.В. Дубов, *Кіберпростір як новий вимір геополітичного суперництва.* Київ, Україна: НІСД, 2014.

[5] Верховна Рада України. 2 сесія. (1994, Лип. 05). *Закон України № 80/94-ВР, Про захист інформації в інформаційно-телекомунікаційних системах*. [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80. Дата звернення: Серп. 21, 2017.

[6] И.Б. Яковив, "Канал связи с позиций атрибутивно-трансферной сущности информации*", Information Technology and Security*, vol. 1, iss. 2, pp. 84-96, 2012.

[7] Верховна Рада України. 7 сесія. (2017, Жовт. 05). *Закон № 2163-19, Про основні засади забезпечення кібербезпеки України*. [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80. Дата звернення: Серп. 21, 2017.

[8] P. Chen, "Chapter 5. A study on Advanced Persistent Threats", in *Communications and Multimedia Security*, L. Desmet, and C. Huygens, Eds. Leuven, Belgium: iMinds-DistriNet, 2014, pp. 63-72.

[9] И.Б. Яковив, "Базовая модель информационных процессов управления и критерии безопасности кибернетической системы*", Information Technology and Security*, vol. 3, iss. 1, pp. 68-73, 2015.

[10] D. Schatz, R. Bashroush, and J. Wall, "Towards a More Representative Definition of Cyber Security", Journal of Digital Forensics, Security and Law, vol. 12 (2*)*. [Online]. Available: https://commons.erau.edu/jdfsl/vol12/iss2/8/. Accessed on: Aug. 21, 2017.

Стаття надійшла до редакції 02 вересня 2017 року.

REFERENCES

[1] International Organization for Standardization. (2012, July 16). ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity.

[2] F. Kramer, S. Starr, and L. Wentz, *Cyberpower and National Security*. Washington, USA: Potomac Books, 2009.

[3] J.B. Sheldon, "Deciphering cyberpower strategic purpose in peace and war", *Strategic Studies Quarterly*, vol. 5, no. 2, pp. 95-112, 2011.

[4] D.V. Dubov, *Cyberspace as a new dimension of geopolitical rivalry*. Kyiv, Ukraine: NISD, 2014.
[5] Verkhovna Rada of Ukraine. 2nd session. (1994, July 05). *Law of Ukraine № 80/94-BP, On the protection of information in information and telecommunication systems*. [Online]. Available: http://zakon3.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80. Accessed on: Aug. 21, 2017.
[6] I.B. Yakoviv, "Communication channel from positions of the attributive-transfer entity of information", *Information Technology and Security*, vol. 1, iss. 2, pp. 84-96, 2012.
[7] Verkhovna Rada of Ukraine. 7th session. (2017, Okt. 05). *Law of Ukraine № 2163-19, About the basic principles of providing cyber security of Ukraine.* [Online]. Available: http://zakon2.rada.gov.ua/laws/show/2163-19. Accessed on: Aug. 21, 2017.
[8] P. Chen, "Chapter 5. A study on Advanced Persistent Threats", in *Communications and Multimedia Security*, L. Desmet, and C. Huygens, Eds. Leuven, Belgium: iMinds-DistriNet, 2014, pp. 63-72.
[9] I.B. Yakoviv, "The base model of informational processes of management and safety criteria for cybernetic systems", *Information Technology and Security*, vol. 3, iss. 1, pp. 68-73, 2015.
[10] D. Schatz, R. Bashroush, and J. Wall, "Towards a More Representative Definition of Cyber Security", Journal of Digital Forensics, Security and Law, vol. 12 (2*)*. [Online]. Available: https://commons.erau.edu/jdfsl/vol12/iss2/8/. Accessed on: Aug. 21, 2017.

ИГОРЬ ЯКОВИВ

ИНФОРМАЦИОННО-ТЕЛЕКОМУНИКАЦИОННАЯ СИСТЕМА, КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ КИБЕРПРОСТРАНСТВА И КИБЕРБЕЗОПАСНОСТЬ

Семантические неопределенности между базовыми понятиями в области кибербезопасности значительно сужают диапазон и снижают результативность научных исследований по методам анализа и прогнозирования, например, APT кибератак или разработки комплексов защиты на основе формальных моделей доказательства их эффективности. Направление возможного решения проблемы – разработка концептуальной модели кибепростору и кибербезопасности, что позволяет снижать уровень возможных неопределенных при описании различных сложных ситуаций в киберпространстве благодаря применению специальных инструментов терминологической, графической и математической формализации. Начало исследований - избранное утверждение: физическую основу киберпространства составляют информационно-телекоммуникационные системы (ИТС). Анализ информационных процессов таких систем было проведено на основе применения атрибутивно-трансферного подхода к сущности информации. Он определяет "информацию" как свойства (атрибуты) объекта, отражающие свойства другого объекта. Электронные устройства и физические среды передачи сигналов составляют технологическую основу ИТС. Дискретные электронные и электромагнитные сигналы, циркулирующие между электронными устройствами, позволяют формировать информацию, преобразовывать ее и передавать в пространстве на разное расстояние. С помощью различных наборов электронных устройств и сигналов в ИТС реализуются различные технологии обработки информации. Они обеспечивают пользователей ИТС различными информационными услугами (сервисами). Пользователями ИТС могут быть как люди, так и технические системы (устройства). По результатам анализа разработана концептуальная модель киберпространства и кибербезопасности. Модель составляют: 1) набор взаимосогласованных базовых терминов, отражающих сущность информационных процессов в ИТС и их составляющих. Благодаря этим терминам синтезированы определения для терминов "киберпространство" и "кибербезопасность"; 2) графическая модель киберпространства, что объясняет соотношение его составляющих; 3) математическая модель киберпространства - набор теоретико-множительных представлений, конкретизирующих характер взаимоотношений между компонентами киберпространства. Благодаря модели киберпространства были разработаны математические критерии кибербезопасности для сегмента киберпостору. Модель также позволяет значительно упростить процесс сценарного анализа APT атак или сложных процессов защиты в киберпространстве.

Ключевые слова: научные исследования APT атак, семантическая неопределенность терминов, информационно-телекоммуникационная система, киберпространство, кибербезопасность, концептуальная модель киберпространства, информационные отношения в киберпространстве, формальные критерии кибербезопасности, сценарный анализ APT атак.

IHOR YAKOVIV

INFORMATION-TELECOMMUNICATION SYSTEM, CONCEPTUAL MODEL OF CYBERSPACE AND CYBERSECURITY

The semantic uncertainties between the basic concepts in the field of cybersecurity significantly narrow the range and reduce the effectiveness of scientific research on methods of analysis and forecasting, for example, APT cyberattacks or the development of security complexes based on formal models of proof their effectiveness. The direction of the possible overcoming of the problem is the development of a conceptual model of cyberspace and cybersecurity, which reduces the level of possible uncertainties in describing various complex situations in cyberspace due to the use of special tools terminology, graphics, and mathematical formalization. The beginning of the research - the selected statement: the physical basis of cyberspace are information and telecommunication systems (ITS). The analysis of the information processes of such systems was carried out on the basis of the attributive-transfer approach to the essence of information. It defines "information" how to get the properties (attributes) of the object, reflecting the properties of another object. Electronic devices and physical environments for signal transmission constitute the technological basis of the ITS. Discrete electronic and electromagnetic signals circulating between electronic devices allow the formation of information, transform it and transmit it in space at different distances. Through various sets of electronic devices and signals in the ITS, various information processing technologies are implemented. They provide ITS users with various information services. Users of ITS can be people or technical systems (devices). According to the results of the analysis, a conceptual model of cyberspace and cybersecurity has been developed. The model consists of: 1) a set of interconnected basic terms that reflect the essence of information processes in the ITS. Due to these terms, synthesized definitions for the terms "cyberspace" and "cybersecurity"; 2) graphic model of cyberspace, which explains the ratio of its components; 3) mathematical model of cyberspace is a collection of mathematical constructions based on the theory of sets that specify the nature of the relationship between components of cyberspace. Cyberspace models have developed mathematical cybersecurity criteria for the cyberspace segment. The model also makes it possible to significantly simplify the process of analyzing APT attacks or complex security processes in cyberspace.

Keywords: APTs research, information-telecommunication system, cyberspace, cybersecurity, semantic uncertainty of terms, conceptual model of cyberspace, information relations in cyberspace, formal cybersecurity criteria, scenario analysis of APTs.

Ігор Богданович Яковів, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та застосування автоматизованих інформаційних систем та технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

E-mail: iyakov52@gmail.com.

Игорь Богданович Яковив, кандидат технических наук, доцент, доцент кафедры кибербезопасности и применения автоматизированных информационных систем и технологий, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.

Ihor Yakoviv, candidate of technical sciences, associate professor, associate professor at the cybersecurity and application of information systems and technology academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.